AUTHENTICATION METHOD FOR COUNTERFEIT PREVENTION, ITS EXECUTION SYSTEM, PROGRAM AND PROGRAM RECORDING MEDIUM

Publication number: JP2004342066
Publication date: 2004-12-02
Inventor: CHU CHIA-CHENG
Applicant: FAST ACCURATE DEVELOPMENTS LTD
Classification:
- international: ***B42D15/10; G06Q50/00; G07F7/08;*** **B42D15/10; G06Q50/00; G07F7/08;** (IPC1-7): B42D15/10; G06F17/60
- European: G06Q30/00C
Application number: JP20030298705 20030822
Priority number(s): TW20030113329 20030516

Also published as:
US 2004230528 (A1)

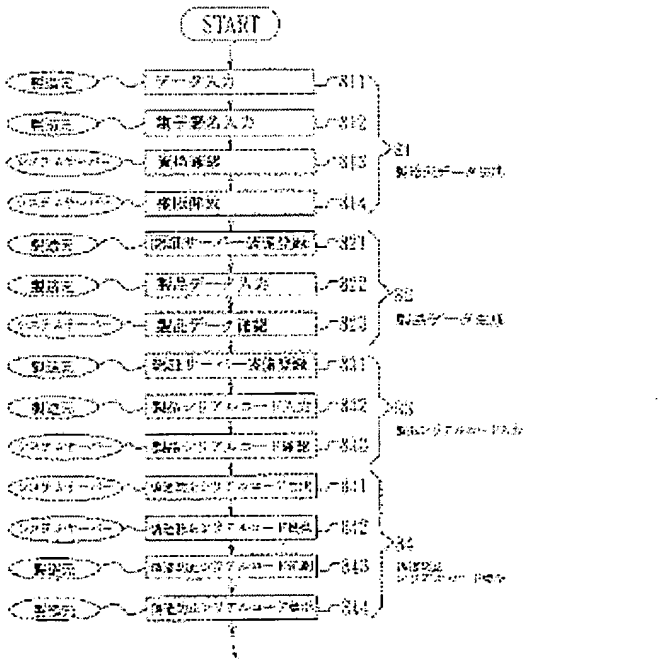
Report a data error here

Abstract of **JP2004342066**

PROBLEM TO BE SOLVED: To provide an authentication method for counterfeit prevention reducing a risk of a consumer to buy a counterfeit.

SOLUTION: This authentication method for counterfeit prevention is provided with a product data input process (822) inputting product data by a manufacturer into authentication server equipment by product, an anti-counterfeit serial code generation process (841) generating a anti-counterfeit serial code corresponding to the product by the authentication server equipment, a serial code providing process (842) providing the anti-counterfeit serial code by the authentication server equipment to label the anti-counterfeit serial code on the product, a shipment/sale data input process inputting shipment/sale data of the product into the authentication server equipment, and a product authentication information providing process providing the product authentication information including at least shipment/sale data of the product corresponding to the anti-counterfeit serial code after receiving an authentication request by the anti-counterfeit serial code from the authentication server equipment.

COPYRIGHT: (C)2005,JPO&NCIPI



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-342066
(P2004-342066A)
(43)公開日　平成16年12月2日(2004.12.2)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 17/60	G06F	17/60	140	2C005
// B42D 15/10	G06F	17/60	154	
	B42D	15/10	501P	

審査請求 有　請求項の数 19　OL　（全 11 頁）

(21)出願番号　特願2003-298705(P2003-298705)
(22)出願日　平成15年8月22日(2003.8.22)
(31)優先権主張番号　92113329
(32)優先日　平成15年5月16日(2003.5.16)
(33)優先権主張国　台湾(TW)

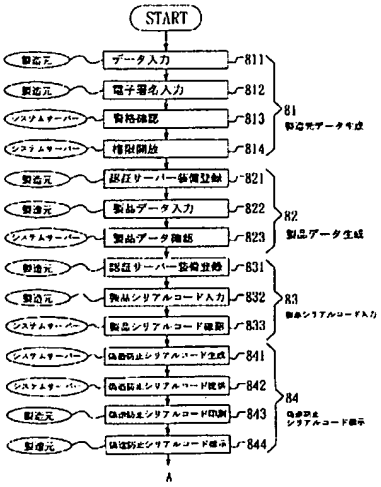
（特許庁注：以下のものは登録商標）
1．フロッピー

(71)出願人　503304186
▲鏡▼準開発有限公司
英国領バージン諸島　トルトーラ　ロード　タウン　オフショア　インコーポレイショナンズ　センター　ビーオー　ボックス　９５７
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　朱　家　正
台湾台北市基隆路１段１１１号９樓

Fターム(参考)　2C005 SA06　SA13

(54)【発明の名称】偽造品防止用認証方法、その実行システム、プログラム及びプログラム記録媒体

(57)【要約】
【課題】消費者が偽造品を買う危険性を低減させる偽造品防止用認証方法を提供する。
【解決手段】偽造品防止用認証方法は、製造元による製品データを製品毎に認証サーバー装備に入力する製品データ入力工程（８２２）と、前記認証サーバー装備により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程（８４１）と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装備により、前記偽造防止シリアルコードを提供するシリアルコード提供工程（８４２）と、前記製品の出荷販売データを前記認証サーバー装備に入力する出荷販売データ入力工程と、前記認証サーバー装備により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備える。
【選択図】　図３



【特許請求の範囲】
【請求項１】
製造元による製品データを製品毎に認証サーバー装備に入力する製品データ入力工程と、
前記認証サーバー装備により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、
前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装備により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、
前記製品の出荷販売データを前記認証サーバー装備に入力する出荷販売データ入力工程と、
前記認証サーバー装備により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備えることを特徴とする偽造品防止用認証方法。
【請求項２】
前記製品データ入力工程は、入力者の資格を確認するための認証を行うステップを第１のステップとして含むことを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項３】
前記製品データ入力工程における製品データは、製造元、製品の名称、仕様、販売区域、製造日、推奨価格、製造地、使用期限、識別コード及び製造元の識別コードからなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項４】
前記製品データ入力工程における製品データは、製品のシリアルコードを含んでおり、前記偽造防止シリアルコード生成工程における偽造防止シリアルコードは、前記製品のシリアルコードに応じて生成することを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項５】
前記製品のシリアルコードは、製造元の識別コード、製品の識別コード、製造元から提供する偽造防止コードからなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項４に記載の偽造品防止用認証方法。
【請求項６】
前記偽造防止シリアルコードは、前記製品のシリアルコードと同一であることを特徴とする請求項４に記載の偽造品防止用認証方法。
【請求項７】
前記出荷販売データ入力工程の後のいずれかの段階に、前記認証サーバー装備によって前記出荷販売データの正否を確認する出荷販売データ確認工程を更に含むことを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項８】
前記出荷販売データ確認工程は、確認者の資格を確認するための認証を行うステップを第１のステップとして含むことを特徴とする請求項７に記載の偽造品防止用認証方法。
【請求項９】
前記出荷販売データ入力工程における出荷販売データは、販売先，販売先の識別コード、製品の出荷日からなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項１０】
前記製品認証情報は、前記製品データを更に含んでいることを特徴とする請求項１に記載の偽造品防止用認証方法。
【請求項１１】
前記製品認証情報は、製造元、製品の名称、仕様、製造日、使用期限、販売先からなる

群より選ばれた少なくとも一つを含んでいることを特徴とする請求項１０に記載の偽造品防止用認証方法。

【請求項１２】

前記製品認証情報提供工程は、前記偽造防止シリアルコードによる認証請求の回数を累計するステップを含むことを特徴とする請求項１に記載の偽造品防止用認証方法。

【請求項１３】

前記製品認証情報提供工程が提供する製品認証情報は、前記偽造防止シリアルコードによる認証請求の回数を含んでいることを特徴とする請求項１２に記載の偽造品防止用認証方法。

【請求項１４】

前記製品認証情報提供工程が提供する製品認証情報は、前記偽造防止シリアルコードによる前回の認証請求日時を含んでいることを特徴とする請求項１３に記載の偽造品防止用認証方法。

【請求項１５】

前記製品認証情報提供工程は、前記偽造防止シリアルコードによる認証請求数が所定以上になると、異常警告を発するステップを含むことを特徴とする請求項１２に記載の偽造品防止用認証方法。

【請求項１６】

製造元を前記製品データ入力工程及び前記販売データ入力工程における入力者とし、

消費者を前記製品認証情報提供工程における認証請求者とし、

販売先を前記出荷販売データ確認工程における確認者とすることを特徴とする請求項１～１５のいずれかの一項に記載の偽造品防止用認証方法。

【請求項１７】

プログラムをロードした認証サーバー装備を備えている偽造品防止用認証システムであって、

前記認証サーバー装備は、前記プログラムに作動されて次の製造元による製品データを製品毎に認証サーバー装備に入力する製品データ入力工程と、

前記認証サーバー装備により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、

前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装備により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、

前記製品の出荷販売データを前記認証サーバー装備に入力する出荷販売データ入力工程と、

前記認証サーバー装備により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程を行うことを特徴とする偽造品防止用認証システム。

【請求項１８】

認証サーバー装備にロードされて前記請求項１～１５のいずれかの一項に記載の偽造品防止用認証方法を前記認証サーバー装備に実行させるためのプログラム。

【請求項１９】

認証サーバー装備にロードされて前記請求項１～１５のいずれかの一項に記載の偽造品防止用認証方法を前記認証サーバー装備に実行させるためのプログラムが記録されている記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、偽造品防止用認証方法、その偽造品防止用認証方法を実行するシステム、その偽造品防止用認証方法を実行するためのプログラム及びそのプログラムを記録する記録媒体に関する。

【背景技術】

【０００２】

一般に、製造元から生産した製品は、認証された販売先や小売りを経由して消費者に販売される。前記販売先や小売りから渡された保証書により、消費者は、買い取った商品が偽造品ではなく、真正品であることを確保することができる。しかしながら、今では、電子交易及びネットワーク市場（サイバー市場）が普及すると共に、商品の偽造技術も日進月歩であると言えるので、消費者としては、前記販売先や小売りでなく他の販売通路から商品（中古品及び平行輸入商品を含む）を取得する時、偽造品を知らずに入手する危険性が非常に高い。また、消費者は、もともと商品の真偽を判断する能力があまりないのが通常であるので、販売先や小売りから保証書を手渡されても、商品の真否を疑う人が少なくない。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

上記に鑑みて、本発明は、消費者が偽造品を買い取る危険性を低減させ、それによって製造メーカや商社の商品販売システム及び名誉を確保することができる偽造品防止用認証方法及びその実行システム、プログラム、プログラム記録媒体を提供することを課題とする。

【課題を解決するための手段】

【０００４】

前記課題を達成するために、まず、製造元による製品データを製品毎に認証サーバー装備に入力する製品データ入力工程と、前記認証サーバー装備により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装備により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、前記製品の出荷販売データを前記認証サーバー装備に入力する出荷販売データ入力工程と、前記認証サーバー装備により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備えることを特徴とする偽造品防止用認証方法を提供する。

【０００５】

それにより、消費者は、製品上の前記偽造防止シリアルコードに基づいて認証請求をし、そして、該製品に関わる認証情報を取った後、買おうとする商品または買い取ったところの商品が偽造品であるか否かを判別することができる。例えば、消費者が、Ａ店に該商品を買ってから家に帰ると、インターネットで前記認証サーバー装備と繋ぎ、該商品に標示されている偽造防止シリアルコードを持って認証請求をし、もし該商品の出荷データにおいてＡ店への出荷が記載されていない場合、該商品は偽造品であると直ぐ判断できる。

【０００６】

そして、また、偽造品防止用認証システムを提供する。該偽造品防止用認証システムは、プログラムをロードした認証サーバー装備を備えているものであって、前記認証サーバー装備は、前記プログラムに作動されて次の、製造元による製品データを製品毎に認証サーバー装備に入力する製品データ入力工程と、前記認証サーバー装備により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装備により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、前記製品の出荷販売データを前記認証サーバー装備に入力する出荷販売データ入力工程と、前記認証サーバー装備により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程を行うことを特徴とする。

【０００７】

さらに、認証サーバー装備にロードされて前記偽造品防止用認証方法を前記認証サーバ

一装備に実行させるためのプログラムを提供する。

さらに、認証サーバー装備にロードされて前記偽造品防止用認証方法を前記認証サーバー装備に実行させるためのプログラムが記録されている記録媒体を提供する。

【発明の効果】

【０００８】

本発明の偽造品防止用認証方法、その実行システム、プログラム及びプログラム記録媒体によれば、消費者は、製品上の前記偽造防止シリアルコードにより認証請求を行って該製品の認証情報を取ることができるので、買おうとする商品または買ったばかりの商品が偽造品であるか否かを判別することができる。したがって、消費者が偽造品を買う危険性を大幅に低減し、製造元または販売商社の販売ルート及び会社の名誉を確保することができる。

【発明を実施するための最良の形態】

【０００９】

以下、本発明の好ましい実施形態を詳しく説明する。この実施形態の偽造品防止用システム１００は、図１に示すように、主として認証サーバー装備１と、製造元で使用される製造元の端末装置２と、販売先で使用される販売先の端末装置３と、認証請求プロキシサーバー４と、消費者に使用される消費者の端末装置５とを備える。製造元及び販売先の端末装置２，３は、それぞれ情報ネットワーク６１，６２を介して認証サーバー装備１と接続されている。消費者の端末装置５は、情報ネットワーク６３及び認証請求プロキシサーバー４を介して認証サーバー装備１と接続されている。それにより、製造元、販売先及び消費者の端末装置２，３，５からデータを認証サーバー装備１に伝送させることができる。

【００１０】

本実施形態における認証サーバー装備１は、分散式フレームワーク構成を有する上、システムサーバー１１と、メインデータベース１２と、バックアップ用データベース１３と、製造元のサーバー１４と、販売先のサーバー１５と、認証請求のサーバー１６とを備える。

【００１１】

システムサーバー１１内には、認証サーバー装備１を管理するに必要な操作システム及び応用プログラムが設けられている。認証サーバー装備１のシステム管理人は、システムサーバー１１により管理を行うことができる。本実施形態において、メインデータベース１２及びバックアップ用データベース１３として、ハードディスクが使用されている。また、それに限らず、メインデータベース１２及びバックアップ用データベース１３として、フロッピーディスクや磁性テープなどの磁気記録媒体、光ディスクなどの光学記録媒体、他の固定式または可動式テープ記録媒体が使用されてもよい。

【００１２】

図２に示すように、メインデータベース１２は、製造元のデータ１２１、製品データ１２２、製品シリアルコード１２３、偽造防止シリアルコード１２４、販売先のデータ１２５、出荷販売データ１２６、製品認証情報１２７、認証請求記録１２８を記憶している。製造元のデータ１２１、製品データ１２２、製品シリアルコード１２３、出荷販売データ１２６は、製造元の端末装置２からメインデータベース１２に送信され、販売先のデータ１２５は、販売先の端末装置３からメインデータベース１２に送信され、偽造防止シリアルコード１２４は、システムサーバー１１からメインデータベース１２に送信される。また、システムサーバー１１から受信した偽造防止シリアルコード１２４は、製造元の端末装置２に送信される。

【００１３】

そして、認証請求記録１２８は、認証請求プロキシサーバー４から前記メインデータベース１２に送信される。該認証請求プロキシサーバー４から受信した認証請求記録１２８は、製造元及び販売先の端末装置２，３に提供される。製品認証情報１２７は、製品データ１２２、出荷販売データ１２６及び認証請求記録１２８から生成し、且つ認証請求プロ

キシサーバー４に提供される。バックアップ用データベース１３は、システムサーバー１１の制御によりメインデータベース１２に記憶されたデータのバックアップを自動かつ定期的に行うように機能する。

【００１４】

なお、図１に示すように、ネットワークの安全性のために、製造元のサーバー１４、販売先のサーバー１５及び認証請求プロキシサーバー４と製造元の端末装置２、販売先の端末装置３及び消費者の端末装置５との間に、外部防火壁７１が設けられている。製造元のサーバー１４、販売先のサーバー１５及び認証請求のサーバー１６とシステムサーバー１１、メインデータベース１２及びバックアップ用データベース１３との間に、内部防火壁７２が設けられている。

【００１５】

外部防火壁７１と内部防火壁７２との間に、認証サーバー装備１を保護して製造元の端末装置２や販売先の端末装置３、消費者の端末装置５からの悪意侵入や攻撃を避ける非武装地帯（ＤＭＺ）７３が形成されている。

【００１６】

前記防火壁の設置は公知技術であり、且つ本発明の特徴と関係がないので、その詳しい説明を省略する。

製造元のサーバー１４、販売先のサーバー１５及び認証請求のサーバー１６は、それぞれ製造元の端末装置２、販売先の端末装置３及び消費者の端末装置５と接続されている。また、製造元のサーバー１４、販売先のサーバー１５及び認証請求のサーバー１６は、メインデータベース１２と接続されている。それにより、端末装置２，３，５からのデータ及び認証請求をサーバー１４，１５，１６を介してメインデータベース１２にアップロードしたり、メインデータベース１２からサーバー１４，１５，１６を介してデータを端末装置２，３，５にダウンロードしたりすることができる。

【００１７】

本実施形態において、製造元の端末装置２及び販売先の端末装置３として、パーソナルコンピューターが使用され、情報ネットワーク６１，６２として、インターネットが使用されているが、それに限らず、情報ネットワーク６１，６２として、例えば、広域ネットワーク（ＷＡＮ）、構内ネットワーク（ＬＡＮ）が使用されてもよい。また、情報ネットワーク６１，６２は、非対称ディジタル加入者線（ＡＤＳＬ）モデム、ダイヤルアップ式モデム、広帯域ケーブルモデムによって、統合ディジタルサービル通信網（ＩＳＤＮ）回線、Ｔ１専用回線、他の有線や無線の接続回線で構築されることができる。

【００１８】

図１に示すように、消費者の端末装置５として、例えば、パーソナルコンピューター５１、携帯用情報端末（ＰＤＡ）５２、携帯電話５３、一般の電話５４、ファックスマシン５５が挙げられる。端末装置５１～５５は、それぞれ有線のインターネット接続６３１、無線のインターネット接続６３２、例えば汎用パケット無線システム（ＧＰＲＳ）及び符号分割多元接続（ＣＤＭＡ）シルテムなどの携帯電話の接続ネットワーク６２３、音声情報伝送用の公衆電話交換網（ＰＳＴＮ）システム６２４、テキスト情報伝送用の公衆電話交換網（ＰＳＴＮ）システム６２５を介して認証請求プロキシサーバー４と接続されている。

【００１９】

前記配置により、消費者（認証請求者）は、任意の場所、任意の時間に各種の端末装置５１～５５を自由に使用し、端末装置５を経由して認証請求を行って製品の認証情報を取得することができる。例えば、パーソナルコンピューター５１または携帯用情報端末（ＰＤＡ）５２により有線または例えばブルートゥースなどの無線の接続を介してオンライン認証請求を行い、携帯電話５３により無線アプリケーション・プロトコル（ＷＡＰ）またはショートメッセージを介して認証請求を行い、一般の電話５４によりキーパッド制御の方式で自動コールアテンダントサービスを介して認証請求を行い、ファックスマシン５５によりテキストの方式でファックス自動回答サービスを介して認証請求を行うことができ

る。

【００２０】

以下、図２～図４を参照しながら、図１のような偽造品防止用認証システムによる偽造品防止用認証方法を説明する。この偽造品防止用認証方法は、主として製造元のデータ１２１を生成する製造元データ生成工程８１と、製品データ１２２を生成する製品データ生成工程８２と、製品シリアルコード１２３を入力する製品シリアルコード入力工程８３と、偽造防止シリアルコード１２４を標示する偽造防止シリアルコード標示工程８４と、販売先のデータ１２５を生成する販売先データ生成工程８５と、製品の出荷販売データ１２６を生成する出荷販売データ生成工程８６と、製品認証請求を行う製品認証請求工程８７とからなる。

【００２１】

製造元データ生成工程８１は、四つのステップ８１１～８１４を有する。まず、製造元は、システム管理者と協力して認証サーバー装備１に登録して製造元のデータ１２１を入力する。製造元のデータ１２１は、メインデータベース１２に記憶される。本実施形態において、製造元のデータ１２１は、製造元の識別コード（ＩＤ、例えばインボイスコード）、パスワード、電子署名、名称、基本資料（例えば電話番号、ファックス番号、ｅメールアドレス、住所アドレスなど）、権限、所在地を含んでいる。そして、製造元は、端末装置２の使用者インターフェイス（例えばインターネットブラウザー）により製造元のサーバー１４を介してメインデータベース１２に入って電子署名を入力する。システムサーバー１１は、製造元の資格を確認する。確認完成後、製造元の権限が開放され、製造元が認証サーバー装備１を操作することができる。

【００２２】

製品データ生成工程８２は、三つのステップ８２１～８２３を有する。まず、製造元は識別コード及びパスワードにより認証サーバー装備１に登録する。登録が成功した後、製品データ１２２を製品毎に認証サーバー装備１に入力する。製品データ１２２は、主として製品の特徴を描く。本実施形態において、製品データ１２２は、製造元、製品の名称、仕様（例えば寸法、重さ、外形、体積、色など）、販売区域、製造日、推奨価格、製造地、使用期限、識別コード及び製造元の識別コードを含んでいる。そして、システムサーバー１１は、製品データ１２２の完成度を確認し、確認した後、メインデータベース１２に記憶する。

【００２３】

製品シリアルコード入力工程８３は、三つのステップ８３１～８３３を有する。まず、製造元は識別コード及びパスワードにより認証サーバー装備１に登録する。登録が成功した後、製品データ１２２と対応する製品シリアルコード１２３を製品毎にメインデータベース１２に入力する。本実施形態において、製品シリアルコード１２３は、製造元の識別コード、製品の識別コード、販売先の識別コード、製造元から提供する偽造防止コード、システムサーバー１１のプログラムから提供する認証コードを含んでいる。そして、システムサーバー１１は、製品シリアルコード１２３の完成度を確認し、確認した後、メインデータベース１２に記憶する。

【００２４】

偽造防止シリアルコード標示工程８４は、四つのステップ８４１～８４３を有する。まず、システムサーバー１１は、製品シリアルコード１２３に応じて偽造防止シリアルコード１２４を生成してメインデータベース１２に記憶する。偽造防止シリアルコード１２４は、製品シリアルコード１２３と完全的または一部的に同じでも良く、製品シリアルコード１２３と特殊的な関係を有する独特の符号、数字、文字及びそれらの組合せでも良い。図５は、偽造防止シリアルコード１２４の一例を示す説明図である。図５中の該偽造防止シリアルコード１２４におけるＭＳ、Ｗ９５、ＴＷ０１、１５２００は、それぞれ製造元の識別コード、製品の識別コード、販売先の識別コード、偽造防止コードを示している。

【００２５】

そして、システムサーバー１１は、前記偽造防止シリアルコード１２４を前記製造元の

端末装置２に送信する。前記製造元は、前記偽造防止シリアルコード１２４を印刷し、対応の製品に標示する。

【００２６】

図６は、図５の偽造防止シリアルコード１２４を製品１０１に標示した時の斜視図である。図６に示すような例は、記図５の偽造防止シリアルコード１２４が空白のラベルに印刷されてから製品１０１上に貼り付けられる方式であるが、それに限らず、マシン読み出し可能のタイプに作ってもよい。

【００２７】

そして、販売先のデータ生成工程８５は、四つのステップ８５１～８５４を有する。まず、販売先は、システム管理者と協力して認証サーバー装備１に登録して販売先のデータ１２５を入力する。販売先のデータ１２５は、メインデータベース１２に記憶される。本実施形態において、販売先のデータ１２５は、販売先の識別コード（ＩＤ、例えばインボイスコード）、パスワード、電子署名、名称、基本資料（例えば電話番号、ファックス番号、ｅメールアドレス、住所アドレスなど）、権限、所在地を含んでいる。そして、販売先は、端末装置３の使用者インターフェイス（例えばインターネットブラウザー）により販売先のサーバー１５を介してメインデータベース１２に入って電子署名を入力する。システムサーバー１１は、販売先の資格を確認する。確認完成後、販売先の権限を開放し、販売先が認証サーバー装備１を操作することができる。

【００２８】

出荷販売データ生成工程８６は、七つのステップ８６１～８６７を有する。製造元は、製品を販売先に出荷した後、製品上の偽造防止シリアルコード１２４により認証サーバー装備１に登録して出荷販売データ１２６を認証サーバー装備１に入力してメインデータベース１２に記憶する。

【００２９】

本実施形態において、出荷販売データ１２６は、製品のシリアルコード、識別コード、製造元の識別コード以外に、販売先，販売先の識別コード、製品の出荷日、製造元の確認シリアルコード、販売先の確認シリアルコード、システムサーバー１１のプログラムに識別される販売確認シリアルコードを含んでいる。そして、製品が入荷した後、販売先は、製品上の偽造防止シリアルコード１２４により製品毎に認証サーバー装備１に登録して対応の出荷販売データ１２６を取り、出荷販売データ１２６の正否を確認する。そして、販売先は、該製品を消費者に販売する。

【００３０】

製品認証請求工程８７は、六つのステップ８７１～８７６を有する。まず、消費者は、認証請求プロキシサーバー４に認証された端末装置５の使用者インターフェイス（例えばインターネットブラウザー）により製品上の偽造防止シリアルコード１２４を入力して認証請求を行う。そして、認証請求プロキシサーバー４はメインデータベース１２から偽造防止シリアルコード１２４と対応する製品認証情報１２７を取得する。

【００３１】

本実施形態において、製品認証情報１２７は、製造元、製品の名称、仕様、製造日、使用期限、販売先、偽造防止シリアルコード１２４による認証請求の累計回数、前記偽造防止シリアルコードによる前回の認証請求日時を含んでいる。

【００３２】

そして、認証請求プロキシサーバー４は、製品認証情報１２７を消費者の端末装置５に提供する。消費者は、製品認証情報１２７に基づいて製品の真偽を判別することができる。例えば、同一の偽造防止シリアルコード１２４による認証請求の回数が異常である時、該製品が偽造される可能性があることが判る。

【００３３】

そして、認証請求プロキシサーバー４は、認証請求記録１２８を自動的に更新すると共に製品認証情報１２７を更新する。本実施形態において、認証請求記録１２８は、製品シリアルコード１２３、認証請求回数、認証請求日時、請求元（例えばＩＰアドレス）、異

常かどうか（偽造防止シリアルコードによる認証請求数が所定以上になる）、製品状況（例えば、製品の現在位置、使用期限）を含んでいる。

【００３４】

次に、認証請求プロキシサーバー４は、認証請求記録１２８を製造元の端末装置２及び販売先の端末装置３に定期的に送信し、製造元及び販売先は、認証請求記録１２８に基づいて偽造の発生があるかどうかを判別することができる。また、偽造防止シリアルコード１２４による認証請求数が所定以上になると、ショートメッセージで製造元及び販売先に異常警告を発するように機能させることもできる。

【産業上の利用可能性】

【００３５】

上記のように、本発明の偽造品防止用認証方法及びその実行システムによれば、消費者が商品の認証情報を容易に取得して商品の真偽を判別することができるので、偽造品を買う危険性を大幅に低減させることができる。また、製造元及び販売先は、前記認証請求記録に基づいて製品が偽造されるかどうかを判別することができるので、商品が偽造される恐れを低減させることができる。即ち、消費者と製造元と販売先との三者の権利を守ることができる。

【００３６】

そして、前記偽造品防止用認証方法及びその実行システムに基づき、本発明は、前記認証サーバー装備にロードされるプログラム及び前記プログラムが記録されている記録媒体を提供することができる。即ち、本発明の偽造品防止用認証システムは、一般のコンピュータ及び今に普及しているインターネットと配合し、低いコストで実行されることができる。

【００３７】

以上説明した実施の形態は、あくまでも本発明の技術的内容を明らかにする意図のものにおいてなされたものであり、本発明はそうした具体例に限定して狭義に解釈されるものではなく、本発明の精神とクレームに述べられた範囲で、いろいろと変更して実施できる。

【図面の簡単な説明】

【００３８】

【図１】本発明の一実施形態にかかる偽造品防止用システムの概略的な構成図。

【図２】メインデータベースと他の装置との関係のブロック図。

【図３】本発明の偽造品防止用認証方法の好ましい実施形態のフローチャート。

【図４】同じく偽造品防止用認証方法の好ましい実施形態のフローチャート。

【図５】偽造防止シリアルコードの一例の説明図。

【図６】図５の偽造防止シリアルコードを製品上に標示した時の斜視図。

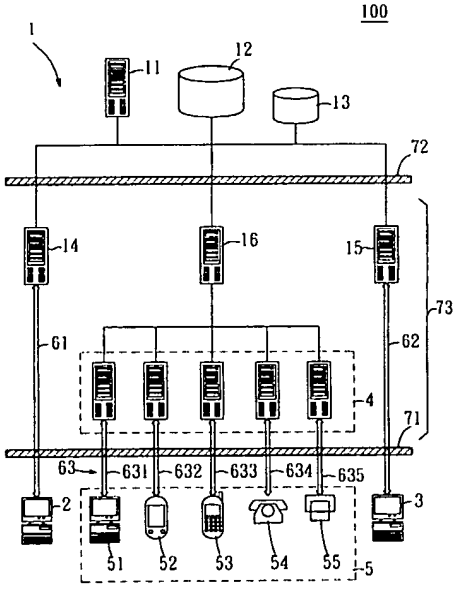
【符号の説明】

【００３９】

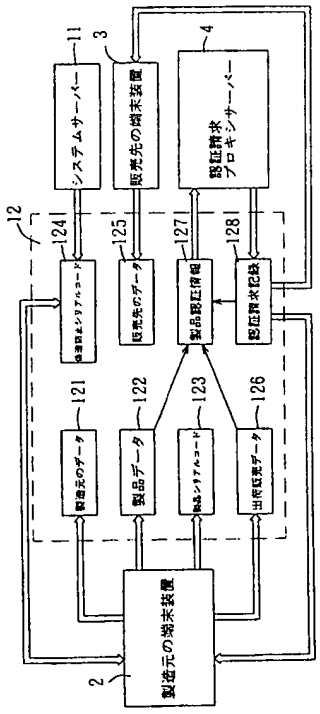
１００　偽造品防止用システム
１０１　製品
１　認証サーバー装備
１１　システムサーバー
１２　メインデータベース
１２１　製造元のデータ
１２２　製品データ
１２３　製品シリアルコード
１２４　偽造防止シリアルコード
１２５　販売先のデータ
１２６　出荷販売データ
１２７　製品認証情報
１２８　認証請求記録

１３　　バックアップ用データベース
１４　　製造元のサーバー
１５　　販売先のサーバー
１６　　認証請求のサーバー
２　　製造元の端末装置
３　　販売先の端末装置
４　　認証請求プロキシサーバー
５，５１～５５　　消費者の端末装置
６１～６３　　情報ネットワーク
６３１～６３５　　情報ネットワック
７１　　外部防火壁
７２　　内部防火壁
７３　　非武装帯域

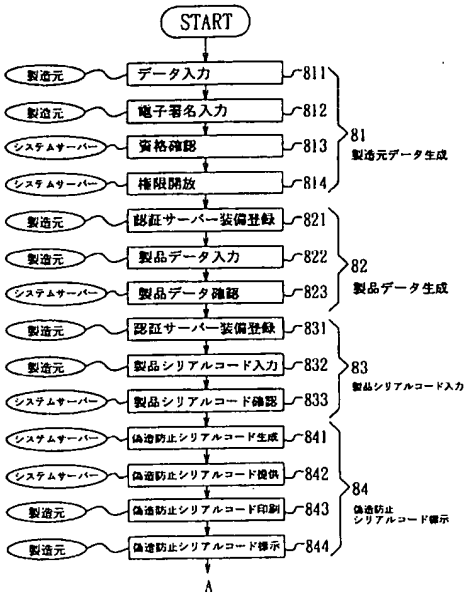
【図１】



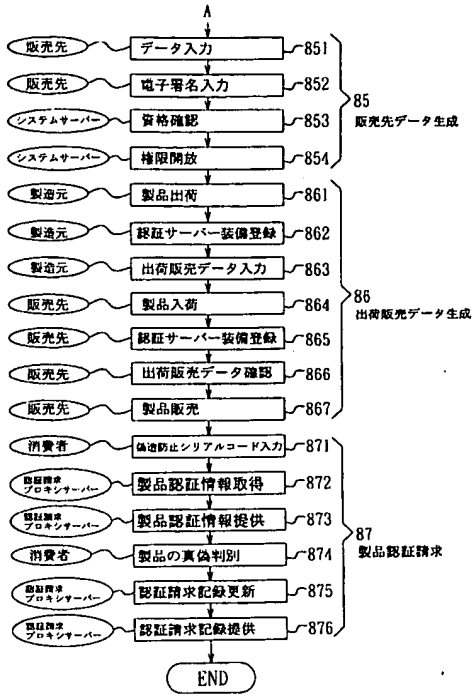
【図２】



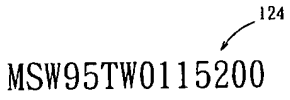
【図３】


START
製造元
データ入力
811
製造元
電子署名入力
812
システムサーバー
資格確認
813
システムサーバー
権限開放
814
81
製造元データ生成
製造元
認証サーバー装備登録
821
製造元
製品データ入力
822
システムサーバー
製品データ確認
823
82
製品データ生成
製造元
認証サーバー装備登録
831
製造元
製品シリアルコード入力
832
システムサーバー
製品シリアルコード確認
833
83
製品シリアルコード入力
システムサーバー
偽造防止シリアルコード生成
841
システムサーバー
偽造防止シリアルコード提供
842
製造元
偽造防止シリアルコード印刷
843
製造元
偽造防止シリアルコード標示
844
84
偽造防止
シリアルコード標示
A

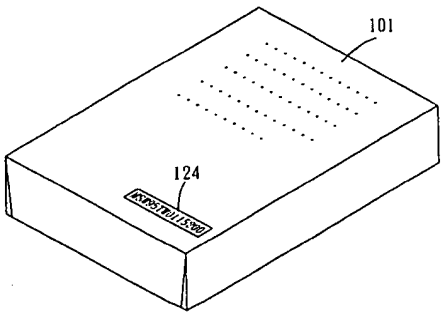
【図４】


A
販売先
データ入力
851
販売先
電子署名入力
852
システムサーバー
資格確認
853
システムサーバー
権限開放
854
85
販売先データ生成
製造元
製品出荷
861
製造元
認証サーバー装備登録
862
製造元
出荷販売データ入力
863
販売先
製品入荷
864
販売先
認証サーバー装備登録
865
販売先
出荷販売データ確認
866
販売先
製品販売
867
86
出荷販売データ生成
消費者
偽造防止シリアルコード入力
871
認証請求
プロキシサーバー
製品認証情報取得
872
認証請求
プロキシサーバー
製品認証情報提供
873
消費者
製品の真偽判別
874
認証請求
プロキシサーバー
認証請求記録更新
875
認証請求
プロキシサーバー
認証請求記録提供
876
87
製品認証請求
END

【図５】


124
MSW95TW0115200

【図６】


101
124
MSW95TW0115200